SCIM WG
Internet-Draft
Intended status: Informational
Expires: April 11, 2013

P. Hunt
Oracle
B. Khasnabish
ZTE USA, Inc.
A. Nadalin
Microsoft
Z. Zeltsan
Alcatel-Lucent
October 8, 2012

SCIM Use Cases
draft-zeltsan-scim-use-cases-00

Abstract

This document lists the use cases of System for Cross-domain Identity Management (SCIM).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 11, 2013.

Copyright Notice

Table of Contents

1. Introduction 3
2. SCIM use cases 3
2.1. Change of the ownership of a file 3
2.2. Migration of the identities 4
2.3. Single Sign-On (SSO) Service 5
2.4. Provisioning of the user accounts for a Community of Interest (CoI) 6
2.5. Update attributes of a user who had previously interacted with a relying party web site 7
2.6. Change notification 8
3. Security considerations 9
4. IANA considerations 9
5. Acknowledgements 9
6. Informative References 9
Authors' Addresses 10

1. Introduction

This document describes the SCIM use cases. It also provides a list of the requirements derived from the use cases. The document's objective is to help with understanding of the design and applicability of SCIM schema [I-D.ietf-scim-core-schema] and SCIM protocol [I-D.ietf-scim-api].

The following section provides the abbreviated descriptions of the use cases.

2. SCIM use cases

This section lists the SCIM use cases.

2.1. Change of the ownership of a file

Description:

Bob - an employee of the company SomeEnterprise - creates a file, which is located at the cloud provided by SomeCSP. After Bob leaves SomeEnterprise, SomeCSP on a request from SomeEnterprise terminates Bob's rights to the file and transfers his former rights to Bill - another employee of SomeEnterprise.

Pre-conditions:

- SomeCSP is a cloud service provider for SomeEnterprise
- With permission of SomeEnterprise, Bob had created a file at the cloud provided by SomeCSP
- Bob has left SomeEnterprise
- SomeEnterprise terminates Bob's rights to the file and, possibly,

decommissions Bob's identity

- SomeEnterprise communicates the changes to the Bob's rights to SomeCSP
- SomeCSP enforces the changes made by SomeEnterprise
- SomeEnterprise requests SomeCSP to transfer Bob's former rights to Bill

Post-conditions:

- Bob does not have the rights to the file at the cloud provided by SomeCSP
- Bill has the rights to the file that Bob had had

Requirements:

- SomeEnterprise can securely communicate to SomeCSP all changes regarding its employee's identity
- SomeCSP can enforce the requested changes
- SomeCSP shall be able to log all changes regarding a SomeEnterprise employee's identity
- The logs should be secure and available for auditing

2.2. Migration of the identities

Description:

A company SomeEnterprise runs an application ManageThem that relies on the identity information about its employees (e.g., identifiers, attributes). The identity information is stored at the cloud provided by SomeCSP. SomeEnterprise has decided to move identity information to the cloud of a different provider - AnotherCSP. In addition, SomeEnterprise has purchased a second application ManageThemMore, which also relies on the identity information. SomeEnterprise is able to move identity information to AnotherCSP

without changing the format of identity information. The application ManageThemMore is able to use the identity information.

Pre-conditions:

- SomeCSP is a cloud service provider for SomeEnterprise
- AnotherCSP is a new cloud service provider for SomeEnterprise
- All involved cloud service providers and applications support the same standard specifying the format for and actions on the user (e.g., employee) identity information

Post-conditions:

- SomeEnterprise has moved its employees' identity information from SomeCSP to AnotherCSP without making any changes to representation of identity information

- Application ManageThemMore is able to use the identity information

Requirements:

- SomeEnterprise, the applications ManageThem and ManageThemMore, the providers SomeCSP and AnotherCSP support a common standard for identity information, which specifies the following:
  - Format (or schema) for representing user identity information
  - Interfaces and protocol for managing user identity information
- Cloud providers shall be able to log all actions related to SomeEnterprise employees' identities
- The logs should be secure and available for auditing

2.3. Single Sign-On (SSO) Service

Description:

Bob has an account with application hosted by a cloud service

provider SomeCSP. SomeCSP has federated its user identities with a cloud service provider AnotherCSP. Bob requests a service from an application running on AnotherCSP. The application running on AnotherCSP, relying on Bob's authentication by SomeCSP and using identity information provided by SomeCSP, serves Bob's request.

Pre-conditions:

- Bob's identity information is stored on SomeCSP
- SomeCSP and AnotherCSP have established trust and federated their user identities
- SomeCSP is able to authenticate Bob
- SomeCSP is able to securely provide the authentication results to AnotherCSP
- SomeCSP is able to securely provide Bob's identity information (e.g., attributes) to AnotherCSP
- AnotherCSP is able to verify information provided by SomeCSP
- SomeCSP is able to process the identity information received from AnotherCSP

Post-conditions:

Bob has received the requested service from an application running on AnotherCSP without having to authenticate to that application explicitly.

Requirements:

- Bob must have an account with SomeCSP
- SomeCSP and AnotherCSP must establish trust and federate their user identities
- SomeCSP must be able to authenticate Bob

- SomeCSP must be able to securely provide the authentication results to AnotherCSP
- SomeCSP must be able to securely provide Bob's identity information (e.g., attributes) to AnotherCSP
- AnotherCSP must be able to verify the identity information provided by SomeCSP
- SomeCSP must be able to process the identity information received from AnotherCSP
- SomeCSP and AnotherCSP must log information generated by Bob's actions according to their policies and the trust agreement between them

2.4. Provisioning of the user accounts for a Community of Interest (CoI)

Description:

Organization YourHR provides Human Resources (HR) services to a Community of Interest (CoI) YourCoI. The HR services are offered as Software-as-a-Service (SaaS) on public and private clouds. YourCoI's offices are located all over the world. Their Information Technology (IT) systems may be composed of the combinations of the applications running on Private and Public clouds along with the traditional IT systems. The local YourCoI offices are responsible for establishing personal information and (i.e., setting the user identities and attributes). YourHR services provide means for provisioning and distributing the employee identity information across all YourCoI offices. YourHR also enables the individual users (e.g., employees) to manage their personal information that they are responsible for

(e.g., update of an address or a telephone number).

Pre-conditions:

- YourCoI has a complex infrastructure composed of the large number of local offices that rely on the diverse IT systems
- YourCoI has contracted YourHR to provide the HR services

- Each local office has a right to establish a personal account for an employee

Post-conditions:

- All personal accounts are globally available to any authorized user or application across the YourCoI system through the services provided by YourHR

- The employees have ability to manage the part of personal information that is in their responsibility

Requirements:

- YourHR must ensure that the personal information generated by the local offices is timely available in a globally-accessible database

- Only authorized users and applications must be able to access personal information

- Identity management of the personal data must be secure

- All operation with identity data must be securely logged

- The logs should be available for auditing

2.5. Update attributes of a user who had previously interacted with a relying party web site

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits relying party web site B, and through a federation protocol (e.g., WS-Federation, SAML, OAuth), selected attributes of the user are transferred from the user's account in directory service A to the web site B at the time of the user's first visit to that site.

The attributes of the user change later in directory service A. For

example, the attributes might change if the user changes their name, has their account disabled, or terminates their relationship with directory service A. The directory service A then wishes to notify relying party web site B of these changes, as relying party B might (or might not) have a cache of those attributes, and if the relying party B were aware of these changes to their cached copy, would potentially cause a state change in relying party B. (E.g., if the user's account were disabled in A, then the relying party B might wish to also change their access control policies as well).

Pre-conditions:

- User has an account in a directory service A
- User has one or more attributes
- User visits web site of a relying party B

Post-conditions:

Selected attributes of the user are transferred from the user's account in directory service A to the web site B at the time of the user's first visit to that site.

Requirements:

Relying parties have to be aware of changes to their cached copy, as these would potentially cause a state change in other relying parties.

2.6. Change notification

Description:

An end user has an account in a directory service A with one or more attributes. That user then visits relying party web site B. Relying party web site B queries directory service A for attributes associated with that user, and related resources.

The attributes of the user change later in directory service A. For example, the attributes might change if the user changes their name, has their account disabled, or terminates their relationship with directory service A. Furthermore, other resources and their attributes might also change. The directory service A then wishes to notify relying party web site B of these changes, as relying party B might (or might not) have a cache of those attributes, and if the relying party B were aware of these changes to their cached copy,

would potentially cause a state change in relying party B.

The volume of changes, however, might be substantial, and only some of the changes may be of interest to relying party B, so directory service A does not wish to "push" all the changes to B. Instead, directory service A wishes to notify B that there are changes potentially of interest, such that B can at an appropriate time subsequently contact directory service A and retrieve just the subset of changes of interest to B.

Pre-conditions:

- User has an account in a directory service A
- User has one or more attributes
- User visits relying party web site B

Post-conditions:

Service A is able to notify B that there are changes potentially of interest.

Requirements:

B must be able at an appropriate time to subsequently contact directory service A and retrieve just the subset of changes of interest to B.

3. Security considerations

TBD

4. IANA considerations

This Internet Draft includes no request to IANA.

5. Acknowledgements

TBD

6. Informative References

Drake, T., Mortimore, C., Ansari, M., Grizzle, K., and E. Wahlstroem, "System for Cross-Domain Identity Management: Protocol", draft-ietf-scim-api-00 (work in progress), August 2012.

[I-D.ietf-scim-core-schema]
Mortimore, C., Harding, P., Madsen, P., and T. Drake, "System for Cross-Domain Identity Management: Core Schema", draft-ietf-scim-core-schema-00 (work in progress), August 2012.

Authors' Addresses

Phil Hunt
Oracle

Email: phil.hunt@oracle.com

Bhumip Khasnabish
ZTE USA, Inc.

Phone: +001-781-752-8003
Email: vumip1@gmail.com, bhumip.khasnabish@zteusa.com

Anthony Nadalin
Microsoft

Email: tonynad@microsoft.com

Zachary Zeltsan
Alcatel-Lucent
600 Mountain Avenue
Murray Hill, New Jersey
USA

Phone: +1 908 582 2359
Email: Zachary.Zeltsan@alcatel-lucent.com